

中国网络安全产业白皮书

（2020 年）

中国信息通信研究院

2020年9月

版权声明

前 言

强大的网络安全产业实力是保障我国网络空间安全的根本和基石。习近平总书记在全国网络安全和信息化工作会议上强调要“积极发展网络安全产业，做到关口前移，防患于未然”，要“抓产业体系建设，在技术、产业、政策上共同发力”，明确了我国产业发展的理念、目标、路径，为网络安全产业发展指明了方向。

近年来，基于政策扶持、需求扩张、应用升级等多方面的驱动，我国网络安全产业发展进入“快车道”。2019 年我国网络安全产业规模较 2018 年增长 17.1%，企业发展态势总体良好，产品体系日益完善，技术创新高度活跃，综合实力显著增强，为保障国家网络空间安全发挥基石力量、做出重要贡献。

此次白皮书是我院第六次发布的中国网络安全产业研究成果。今年白皮书紧密跟踪国内外网络安全产业发展动态，重点关注产业综合现状，除了延续从规模结构、政府政策、企业发展、人才培养等维度对国内外产业发展进行跟踪之外，还结合新冠疫情等热点事件对我国产业发展进行现状分析和前景展望。后续将进一步对我国网络安全企业情况进行研究，并结合热点技术趋势，对 5G 安全、车联网安全、“区块链+安全”、容器安全、数据合规等五个领域进行分析预测。希望为关注网络安全产业发展的企业、政府机构以及相关单位提供参考和帮助。

在本白皮书的研究过程中，得到以下单位的支持协助，在此表示

感谢（以企业名称笔画为序）：山石网科通信技术股份有限公司、上海观安信息技术股份有限公司、上海纽盾科技股份有限公司、上海银基信息安全技术股份有限公司、中兴通讯股份有限公司、中国电子科技网络信息安全有限公司、天津市国瑞数码安全系统股份有限公司、北京天融信网络安全技术有限公司、北京升鑫网络科技有限公司（青藤）、北京安天网络安全技术有限公司、北京安信天行科技有限公司、北京安博通科技股份有限公司、北京启明星辰信息安全技术有限公司、北京芯盾时代科技有限公司、北京奇虎科技有限公司、北京知道创宇信息技术股份有限公司、北京神州绿盟科技有限公司、北京梆梆安全科技有限公司、北京智游网安科技有限公司、北京微智信业科技有限公司、北京酷德啄木鸟信息技术有限公司、北京蔷薇灵动科技有限公司、华为技术有限公司、江苏易安联网络技术有限公司、江苏通付盾信息安全技术有限公司、亚信安全科技有限公司、华信咨询设计研究院有限公司、杭州安恒信息技术股份有限公司、杭州美创科技有限公司、奇安信科技集团股份有限公司、杭州默安科技有限公司、重庆贝特计算机系统工程有限公司、恒安嘉新（北京）科技股份公司、浙江鹏信信息科技股份有限公司。

目 录

图 目 录

表 目 录



一、全球网络安全产业规模

（一）全球网络安全产业规模增长放缓

2019 年全球网络安全产业规模达到 1244.01 亿美元，预计 2020 年增长至 1278.27 亿美元[1]。从增速上看，2019 年全球网络安全产业增速为 9.11%，达到自 2014 年以来最低值；受疫情影响，2020 年最新预期增速远低于 2019 年 12 月的预测值，约为 2.75%。2014-2020 年全球网络安全产业规模及增速如图 1 所示。

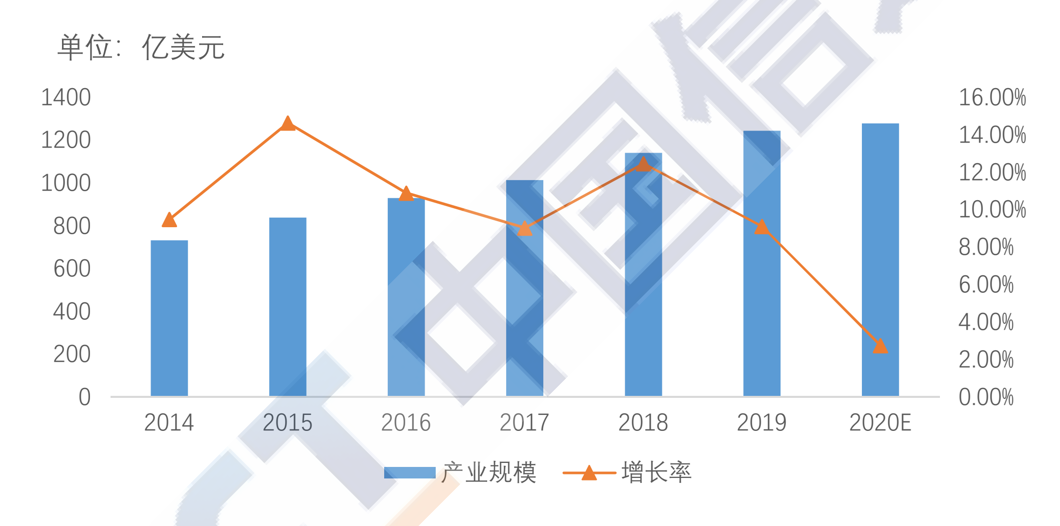


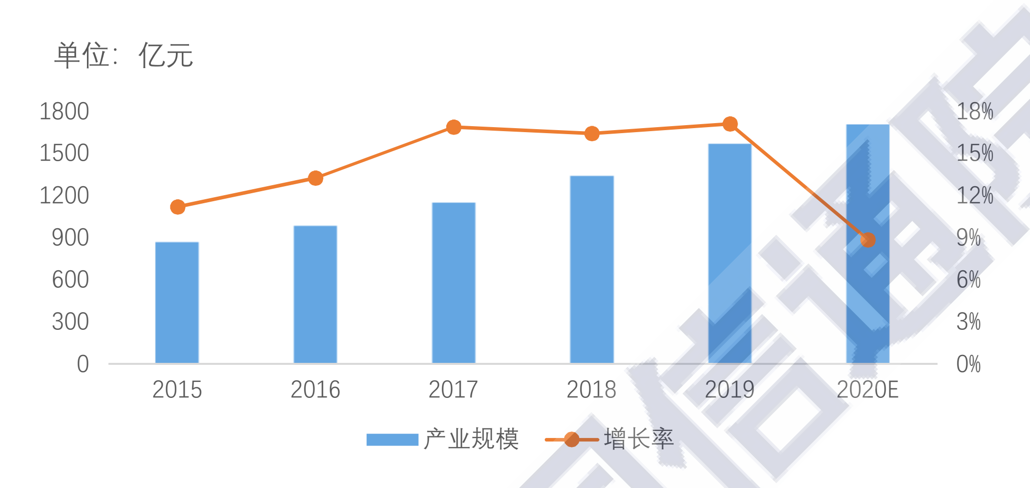
图 1　2014-2020 年全球网络安全产业规模及增速

（二）我国产业规模呈现持续高速增长态势

随着新一代信息技术的融合发展，对网络空间安全的认知不断深化，为真实、全面地反映产业发展现状，**本次测算对网络安全产业范畴进行了扩充，将例如区块链应用等安全新技术产品、密码产品和设备等信息安全产品纳入考量范围，同时将云服务企业、电信运营商、车联网企业等主体的网络安全业务也纳入计算范围。**

[1] 数据来源：Gartner, Information Security and Risk Management, Worldwide, 2018-2024, 2Q20 Update

根据新的统计测算，2019 年我国网络安全产业规模达到 1563.59 亿元，较 2018 年增长 17.1%，预计 2020 年产业规模约为 1702 亿元，增速约为 8.85%。2015-2020 年我国网络安全产业规模增长情况如图 2 所示。



数据来源：中国信息通信研究院

图 2　2015-2020 年我国网络安全产业规模增长情况[2]

二、全球网络安全产业进展

（一）国际网络安全政策措施持续优化

立足全球网络空间安全的总体形势，各国网络安全政策主要聚焦于确保在 5G[3]、人工智能等未来技术创新领域中的领先地位。

1. 美国频繁发布网络安全政策，大量增加网络安全投入

美国通过加大网络安全投入、引导技术创新方向、强化供应链安全等系列措施，为产业释放红利，夯实网络安全产业基础。**网络安全投入方面**，2020 年 2 月，美国白宫 2021 财年预算提案包括约 188 亿

[2] 说明：已基于新的网络安全产业范畴对往年数据进行追溯调整

[3] 5G：Fifth-Generation Mobile Networks，第五代移动通信

美元的网络安全经费；2020 年 7 月，美国国土安全部发布 2020-2024 财年战略计划概要，将网络空间和关键基础设施安全作为重要目标之一。**信息通信新技术领域安全方面**，2020 年初，美国先后发布《促进美国 5G 国际领导力法案》《促进美国无线领导力法案》《保障 5G 安全及其他法案》《5G 安全国家战略》等一系列政策，旨在引导美国研发、部署和管理安全可靠的 5G 通信基础设施，提高美国在国际电信界的声誉和领导地位。**网络安全技术创新方面**，2019 年至今，美国针对零信任技术、对抗机器学习等先进网络安全技术进行持续探索，先后形成《零信任架构》《对抗性机器学习的分类和术语》《基于域名解析系统的邮件安全实践指南》等阶段性研究成果，指导构建新一代网络安全防护体系。**供应链安全方面**，2020 年 3 月，NIST[4]下属国家网络安全卓越中心（NCCoE[5]）发布名为《供应链安全保障 验证计算设备完整性》的报告，旨在协助企业和用户应对供应链安全风险。

2. 欧盟重点聚焦新兴科技领域，捍卫网络安全领跑地位

欧盟在前期网络安全一揽子计划的基础上，针对新技术应用领域重点发力，以期在欧盟层面形成整体合力，努力使欧洲成为全球网络安全的引领者。**5G 安全方面**，2019 年 10 月起，欧盟先后发布《欧盟 5G 网络安全风险评估》《5G 网络的威胁状况》《5G 网络的威胁状况》《5G 网络安全风险缓解措施工具箱》等系列文件和指南，持续推进 5G 安全风险评估。**人工智能方面**，欧盟发布《人工智能白皮书》，

[4] NIST：National Institute of Standards and Technology，美国国家标准与技术研究院
[5] NCCoE：National Cybersecurity Center of Excellence，美国国家网络安全卓越中心

旨在构建一个卓越、可信赖的人工智能体系框架。

3. 俄罗斯探索一系列强化措施，保障本国网络安全发展

俄罗斯致力于维护俄罗斯网络空间权益，积极探索对网络主权管辖的保护途径。**强化本国互联网韧性方面**。2019年11月，俄罗斯《主权互联网法》正式生效，从域名自主、定期演练、平台管控、主动断网、技术统筹五方面捍卫“自主可控”国家网络主权，并在12月完成了外部“断网”测试演习。**数据安全风险管理方面**。2019年12月，俄罗斯实施第405号联邦法律，要求两年内禁止州和市政府购买外国供应商的数据存储系统，以确保国家关键IT[6]基础架构的安全。

4. 韩国发力新兴产业领域发展，不断完善安全支撑机制

韩国近年来频繁发布新兴产业领域政策规范。**5G方面**，2019年11月，韩国政府出台《国家网络安全基本规划》，以应对5G超级互联社会发展所面临的国家网络安全风险，增强民官军联合应对体系。2020年1月，韩国科学与信息通信技术部发布了该国2020年推进5G发展的政策举措。**人工智能方面**，2020年1月，韩国科技部公布2020年度工作计划，正式启动《人工智能国家战略》。

（二）网络安全细分市场格局稳中有变

1. 美欧亚地区保持三足鼎立格局

在地区分布方面，北美地区继续占据全球网络安全市场的最大份

[6] IT：Internet Technology，互联网技术

额，其次仍然为西欧和亚太地区。其中，以美国、加拿大为主的北美地区 2019 年网络安全市场规模为 581.75 亿美元，较 2018 年增长 11.87%，增速超过西欧地区跃居全球第一。以英国、德国、芬兰等国为主的西欧地区网络安全市场规模为 306.79 亿美元，较 2018 年增长 5.43%。中国、日本、澳大利亚等亚太地区网络安全市场规模为 268.09 亿美元，较 2018 年增长 8.62%。2019 年全球网络安全产业区域分布情况如图 3 所示。

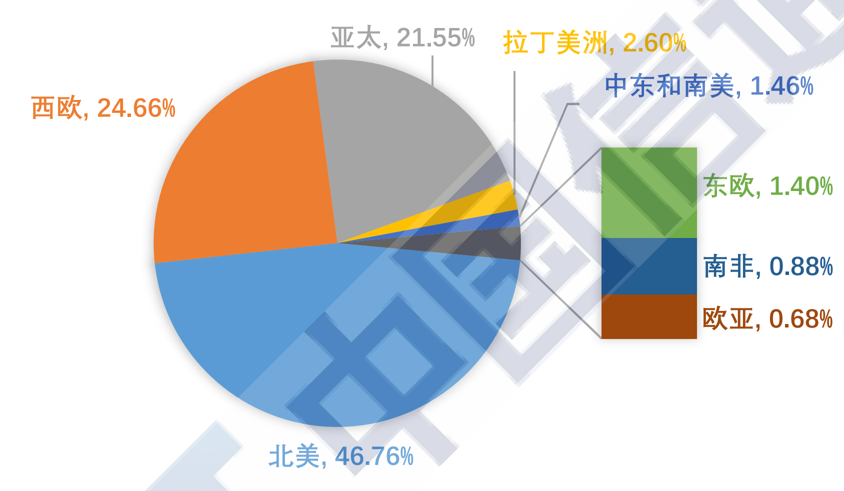


图 3　2019 年全球网络安全产业区域分布情况

2. 国际市场安全服务与产品市场趋于五五分

根据 Gartner 统计数据，全球网络安全服务市场与安全产品市场格局逐步逼近五五分。其中，近三年来网络安全产品市场占比逐步提升，并于 2019 年首次超过网络安全服务市场，达到 50.22%，如图 4 所示。

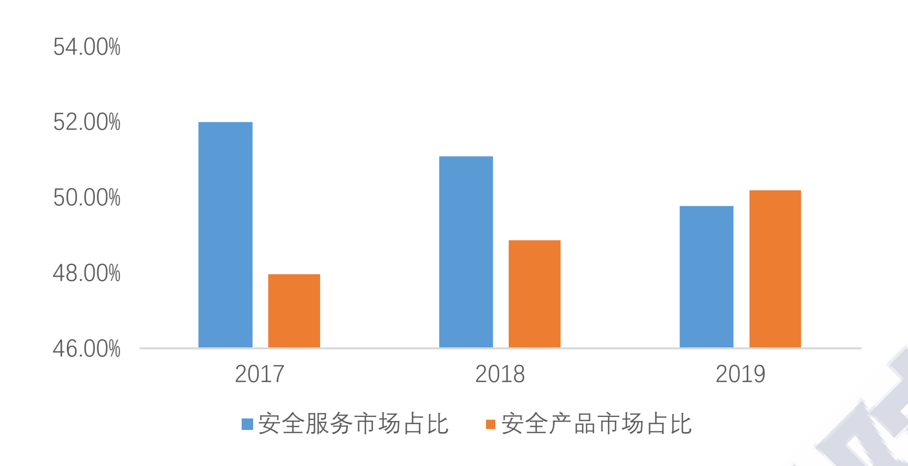


图 4　2017-2019 年全球网络安全产品/服务市场占比

2019 年全球网络安全服务市场规模为 619.22 亿美元，较 2018 年增长 6.30%，安全托管服务（MSS[7]）、安全咨询服务市场份额分别为：18.73%、36.90%，如图 5 所示。

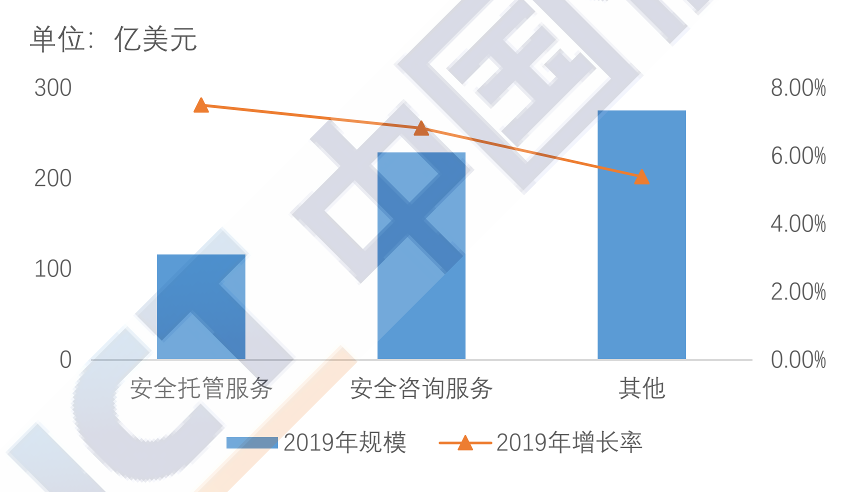


图 5　2019 年全球网络安全服务市场规模及增长情况

在**安全托管服务**方面，市场规模达到 115.96 亿美元，相比 2018 年增长 7.49%。新兴服务业的兴起推动安全托管市场的持续发展，其中，市场规模最大的五家供应商分别为 IBM[8]、AT&T[9]、Atos[10]、

[7] MSSP: Managed Security Services，可管理安全服务
[8] IBM：International Business Machines Corporation，国际商业机器公司
[9] AT&T：总部位于美国，成立于 1877 年，电信公司
[10] Atos：源讯，总部位于法国，信息技术服务公司

Secureworks[11]和 DXC[12]，市场占有率分别达到了 4.8%、3.9%、3.8%、3.5%和 3.4%[13]。在**安全咨询服务**方面，市场规模达到 228.52 亿美元，相比 2018 年增长 6.81%。北美地区占据全球市场最大份额，达到 45.2%，较 2018 年增长 7.5%；西欧地区占据全球市场份额为 45.2%，较 2018 年增长 6.1%；亚太地区占据全球市场份额为 16.1%，较 2018 年增长 6.0%[14]。

2019 年全球网络安全产品市场规模达到 624.78 亿美元，较 2018 年增长 12.06%。市场份额最高的三类依次是基础设施保护、网络安全设备、身份管理。其中，基础设施保护类产品的市场规模为 188 亿美元，占比为 30.01%；网络安全设备类产品的市场规模为 134 亿美元，占比为 21.43%；身份管理类产品的市场规模为 110 亿美元，占比为 17.61%，如图 6 所示。

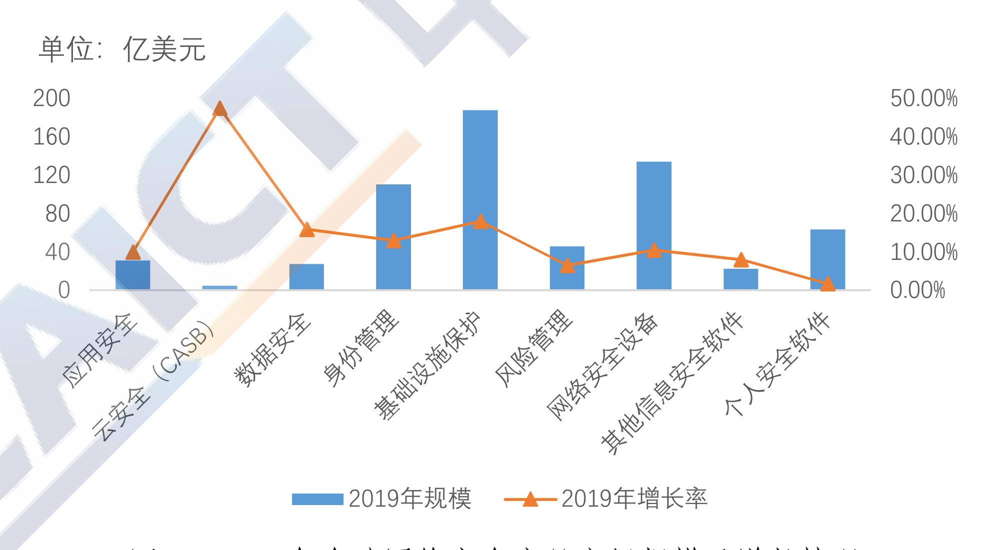


图 6　2019 年全球网络安全产品市场规模及增长情况

增速方面，排名前三的网络安全产品类别仍然是云访问安全代理

[11] Secureworks：总部位于美国，信息安全服务厂商
[12] DXC：总部位于美国，端到端 IT 服务公司
[13] 数据来源：Gartner, Market Share: Managed Security Services, Worldwide, 2019
[14] 数据来源：Gartner, Market Share: Security Consulting Services, Worldwide, 2019

（CASB[15]）、基础设施保护和数据安全。其中，云访问安全代理产品市场增速达到 47.45%；云计算市场的持续扩张和安全事件的不断频发，共同推动了云安全市场包括 CASB 在内的相关产品市场快速增长。基础设施保护产品市场增速达到 17.97%；各国针对基础设施安全法案、文件的不断提出，刺激了基础设施保护产品市场的增长。数据安全产品市场增速达到 15.85%；各国不断推出的隐私安全等合规要求驱动企业积极部署数据防泄漏、数据管控等相关产品。

（三）上市企业发展态势两级分化

1. 企业营收及盈利能力分化加剧

在营收方面，2019 年上市网络安全企业营收保持普涨态势，营收增速差距持续扩大。包括 CheckPoint[16]、Norton Life Lock[17]、Palo Alto Networks[18] 等在内的 10 家典型网络安全企业平均营收为 17.44 亿美元，较 2018 年增长 12.81%，平均营收增幅较 2018 年度小幅上升。其中，Splunk[19]、Palo Alto Networks、CyberArk[20]营收增速分别为 41.86%、27.58%、26.53%，而 Norton Life Lock、Check Point[21]、FireEye[22]等厂商增速低迷，其中 Norton Life Lock 呈现负增长。2017-2019 年国际主要上市网络安全企业营收情况如图 7 所示。

[15] CASB：Cloud Access Security Broker，云访问安全代理
[16] CheckPoint：总部位于以色列特拉维夫，网络安全解决方案供应商
[17] Norton Life Lock：诺顿，总部位于美国，信息安全解决方案提供商
[18] Palo Alto Networks：派拓网络，创立于 2005 年
[19] Splunk：成立于 2003 年，全球知名大数据公司
[20] CyberArk：赛博埃克，安全软件公司
[21] Check Point：总部位于以色列特拉维夫，网络安全解决方案供应商
[22] FireEye：火眼，总部位于美国

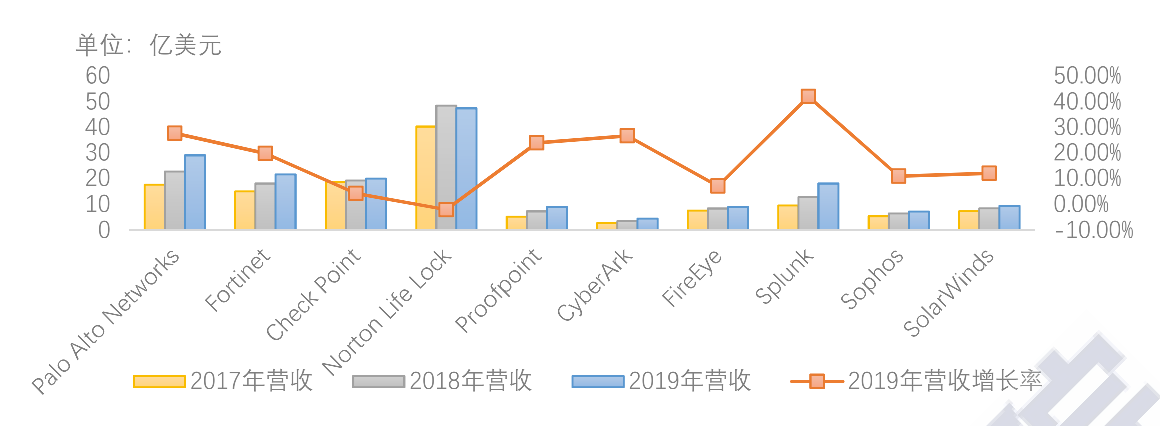


图 7　2017-2019 年国际主要上市网络安全企业营收情况

在净利润方面，上市网络安全企业呈现盈亏并存局面。2019 年，9 家典型网络安全企业平均净利润为 0.574 亿美元[23]，相较于 2018 年大幅增加 86%。其中，Splunk、Palo Alto Networks、Proofpoint[24]、FireEye 等企业净利润持续告负，Sophos[25]和 SolarWinds[26]则实现了由亏转盈的转变。2017-2019 年国际主要上市网络安全企业净利润情况如图 8 所示。

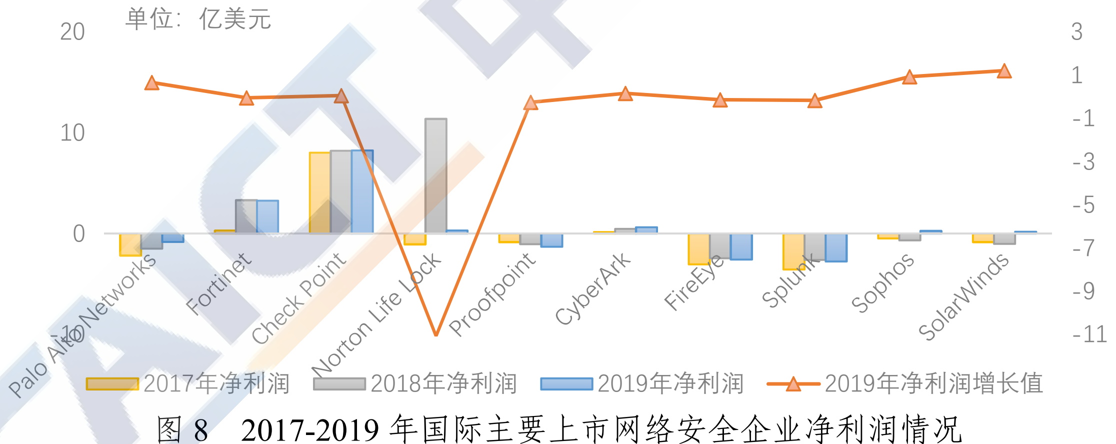


图 8　2017-2019 年国际主要上市网络安全企业净利润情况

在研发投入方面，2019 年上市网络安全企业研发投入普涨，研发投入占营收比例保持高位。10 家典型网络安全企业的平均研发投入

[23] 说明：Palo Alto Networks 盈利及增速情况在行业中较为特殊，故计算平均净利润时未将其纳入
[24] Proofpoint：证据点，美国著名网络安全公司
[25] Sophos：守护使，IT 安全与保护公司
[26] SolarWinds：创立于 1999 年，总部位于美国

增长为 13.53%，占营收比例为 18.57%，略高于 2018 年的 18.45%。其中 Norton Life Lock 研发投入略有降低，但仍保持在 9 亿美元高位，远超其他厂商。Palo Alto Networks 研发投入增加了 34.66%至 5.4 亿美元，位列第二；Splunk 研发投入增长了 46.84%至 4.4 亿美元，位列第三；其余企业未超过 3 亿美元。2017-2019 年国际主要上市网络安全企业研发投入情况如图 9 所示。

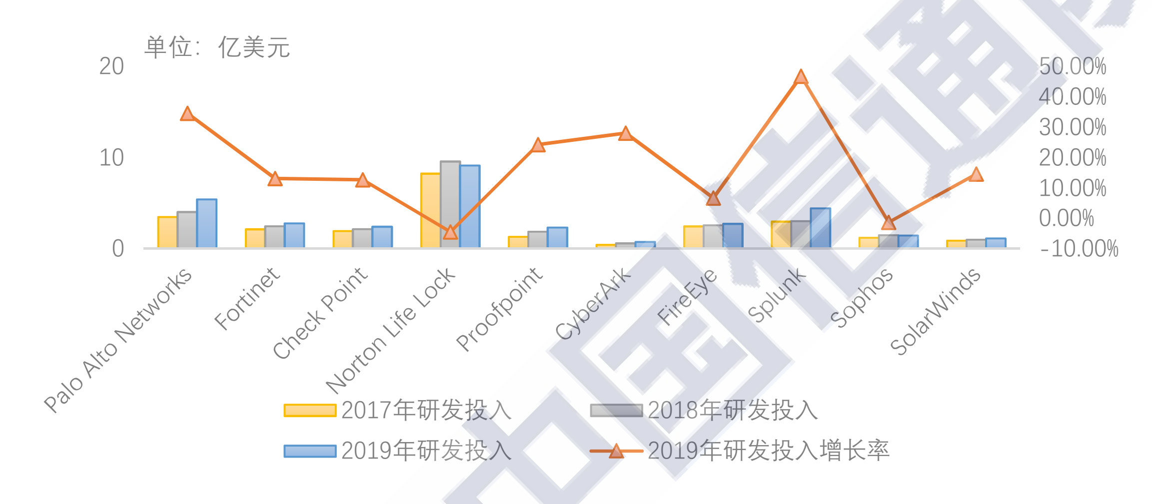


图 9　2017-2019 年国际主要上市网络安全企业研发投入情况

2. 网络安全新上市企业表现强劲

据不完全统计，2019 年有 4 起网络安全 IPO[27]，较 2018 年减少了 1 起。2019 年 IPO 的平均融资额为 3.81 亿美元。2019 年国际网络安全企业 IPO 情况如表 1 所示。

表 1　2019 年国际网络安全企业 IPO 情况

上市时间	企业名称	技术领域	上市场所
2019.04	Tufin	安全策略管理	纽约证券交易所
2019.06	Crowdstrike	终端安全	纳斯达克交易所
2019.09	Cloudflare	内容分发网络和安全服务	纽约证券交易所
2019.09	Ping identity	身份管理	纽约证券交易所

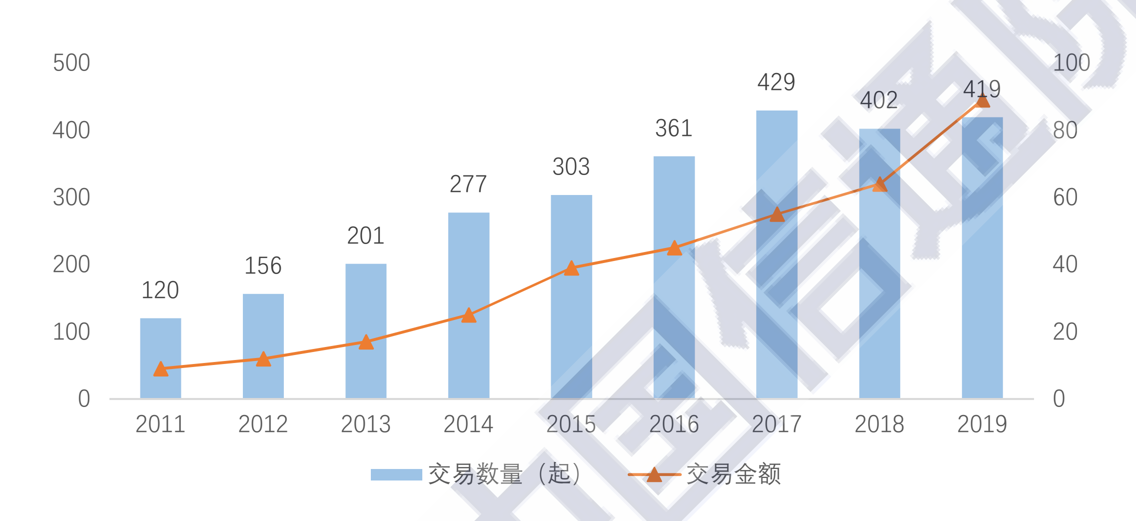
来源：中国信息通信研究院根据公开资料整理

[27] IPO：Initial Public Offering，首次公开募股

（四）网络安全融资并购活动持续活跃

1. 融资数量小幅提高，交易总额持续增长

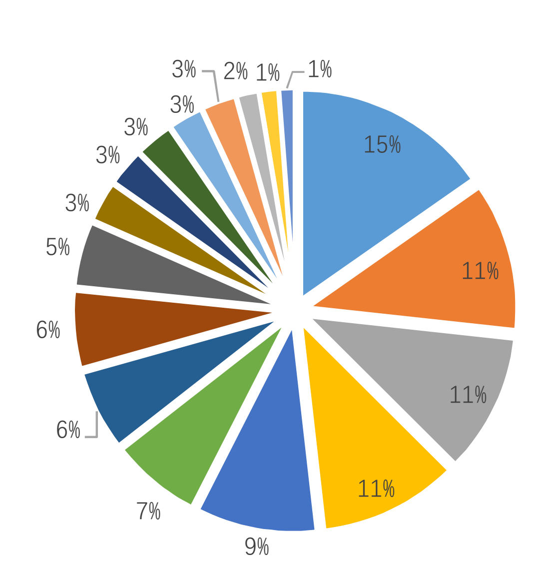
2019 年，全球网络安全融资活动为 419 起，较 2018 年的 402 起小幅提高 4.23%；交易额达到 89 亿美元，较 2018 年增长 39%，如图 10 所示。



数据来源：Momentum Cyber

图 10　2011-2019 年网络安全初创企业融资态势

从融资的技术领域来看，数据安全、身份管理与访问控制、网络与基础设施安全、风险管理与合规等领域融合活动占比均超过 10%，融资数量分别达到 45 起、45 起、48 起、64 起。从融资轮次分布看，2019 年共有 148 家的企业位于天使轮阶段，交易总额为 5 亿美元；处于 A 轮的企业有 94 家，交易总额为 15 亿美元；有 53 家企业处于 B 轮阶段，交易总额为 13 亿美元；位于 C+轮的有 109 家，交易总额为 55 亿美元。C+轮的交易数量和交易额分别占总额的 26%和 62%，显示市场对较为成熟型的企业更为看好。2019 年全球网络安全融资领域分布情况如图 11 所示。

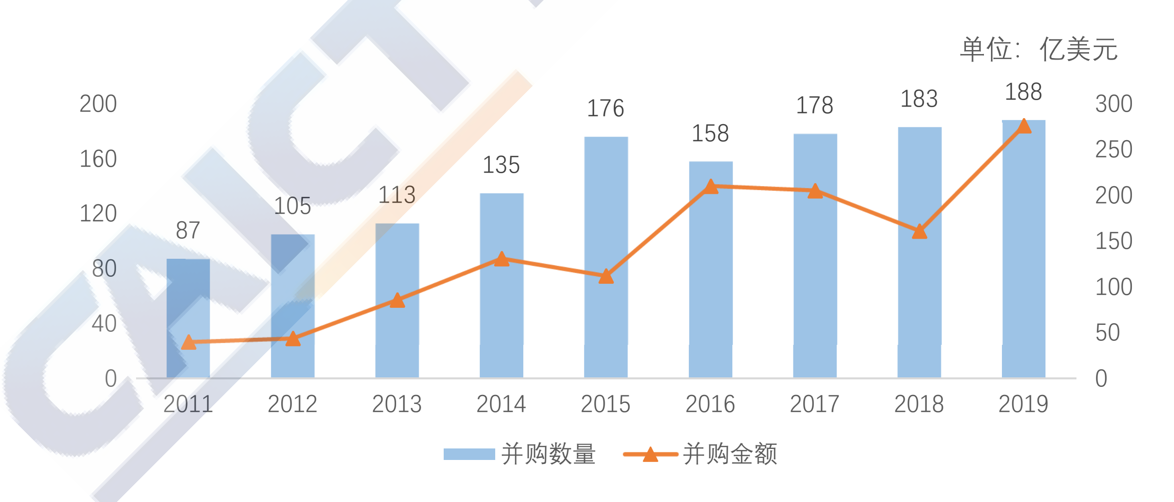


数据来源：Momentum Cyber

图 11　2019 年全球网络安全融资领域分布情况

2. 并购数量再创新高，热点领域发生变化

据不完全统计，2019 年全球共完成了 188 起并购活动，较 2018 年小幅提升，处于历史最高位水平；交易额为 276 亿美元，较 2018 年的大幅提高 78.06%，如图 12 所示。



数据来源：Momentum Cyber

图 12　2011-2019 年全球网络安全并购活动态势

从并购的技术领域来看，安全托管服务和安全咨询与服务领域成为了 2019 年最热门的选择，并购活动占比均达到约 16.5%。一方面，

安全托管服务领域共有 31 起并购活动，比 2018 年的 15 起增加了约 107%；WEB 安全、消息安全和物联网安全等领域并购活动数量也有所增加，分别较 2018 年增加了 7、5、4 起。另一方面，身份管理与访问控制、安全运营/应急响应/互联网威胁等领域并购活动数量出现回落，较 2018 年分别减少 14、12 起，减幅达到约 45%、52%。2019 年全球网络安全并购领域分布情况如图 13 所示。

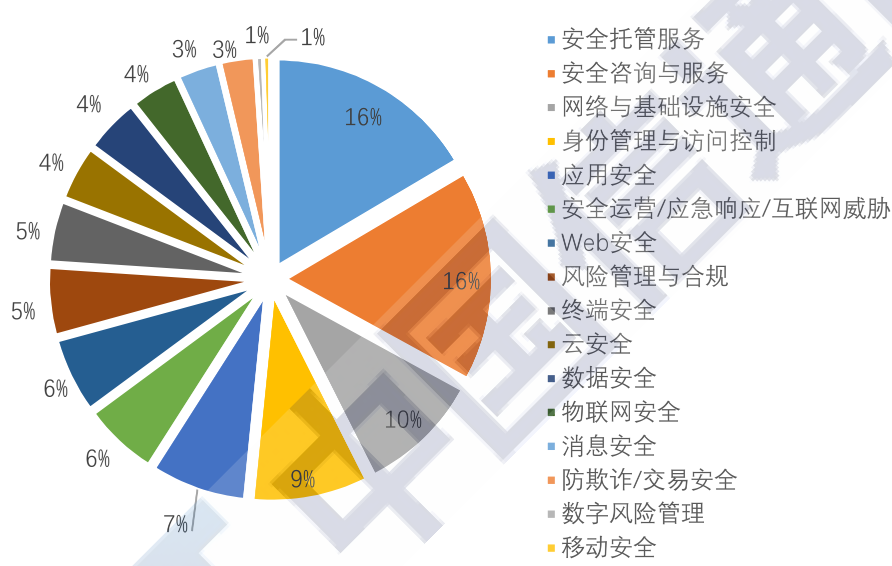


图 13　2019 年全球网络安全并购领域分布情况

从并购交易方看，2019 年安全企业积极通过并购实现能力拓展，如 Palo Alto Networks 领导并购活动，共完成了 5 起交易，总金额达 12 亿美元；Akamai[28]、Check Point 等网络安全企业也都完成了 3 起收购。此外，2019 年值得关注的典型网络安全并购活动如表 2 所示。

[28] Akamai：阿卡迈，CDN 服务提供商

表 2　2019 年值得关注的网络安全并购活动[29]

日期	被收购方	并购方	技术领域	金额（亿美元）
2019.8	Symantec	Broadcom	网络安全	107.00
2019.10	Sophos	Thomabravo	网络安全	39.48
2019.8	Carbon Black	VMware	终端安全	21.00
2019.11	Carbonite	Opentext	数据安全	13.96
2019.12	Shape	F5	应用安全	10.00

来源：中国信息通信研究院根据公开资料整理

三、我国网络安全产业进展

（一）网络安全政策措施不断出台

我国网络安全相关政策布局仍在不断提速，积极推动网络安全及相关政策出台，为促进产业发展提供了良好的政策保障。

1. 网络安全政策规范稳步推进

一是网络安全法律及配套政策密集落地，安全合规市场空间得到了拓展。2019 年 12 月，网络安全等级保护 2.0 相关国家标准正式实施，为网络安全等级保护制度的落地提供了标准支撑。2020 年 1 月，《中华人民共和国密码法》正式施行，为我国商用密码技术和产业的发展开放平台。**二是网络法制建设继续稳步推进，持续拉动产业规模发展。**《个人信息保护法》《数据安全法》已纳入 2020 年立法计划，两部法律的制定将推动我国个人信息和数据安全保护进入全新阶段。**三是围绕网络安全产业发展，更多政策指引陆续出台落地。**2019 年 9 月工信部《关于促进网络安全产业发展的指导意见(征求意见稿)》公

[29] 说明：表格中日期为交易意向披露或成交完成日期

开征求意见，提出“到 2025 年，培育形成一批年营收超过 20 亿的网络安全企业，形成若干具有国际竞争力的网络安全骨干企业，网络安全产业规模超过 2000 亿”的发展目标。

2. 新兴领域政策举措密集落地

一是引导网络安全与新技术融合应用的发展方向。2020 年以来，工业和信息化部印发的《国家车联网产业标准体系建设指南(车辆智能管理)》《关于推动 5G 加快发展的通知》《关于推动工业互联网加快发展的通知》，以及国家标准化管理委员会等五部门联合发布的《国家新一代人工智能标准体系建设指南》等政策指引，聚焦新一代前瞻性技术创新，加快完善新兴技术的网络安全产品和服务支撑体系，为产业奠定长期发展的政策基础。**二是结合新兴技术特征出台针对性安全政策。**随着等保 2.0 制度将等级保护对象范围扩大到云计算、物联网、大数据等领域，新兴技术安全政策加速落地。2019 年 9 月，国家网信办等四部门联合发布的《云计算服务安全评估办法》正式施行，旨在降低党政机关、关键信息基础设施运营者采购使用云计算服务带来的网络安全风险。2019 年 12 月，工业和信息化部发布《工业互联网企业网络安全分类分级指南（试行）》（征求意见稿），着力提升工业互联网安全保障能力和水平。

3. 地方政府加速网络安全领域布局

一是各省相继公布 5G 安全发展推进政策。2019 年至今，已有近 30 个省发布了 5G 产业推动计划，如 8 月河北省出台《关于加快 5G

发展的意见》。2019年9月上海发布《上海5G产业发展和应用创新三年行动计划(2019-2021年)》。2020年2月湖南省发布《加快第五代移动通信产业发展的若干政策》等，其中超20个省明确提及，强化网络信息安全保障，推动5G与网络安全产业融合，对于推动5G安全的落地和推广具有重要作用。**二是多地陆续出台网络安全产业促进政策**。2019年下半年以来，多地积极推动网络安全相关产业促进政策出台，为产业发展指明重点及方向。2020年3月《成都市加快网络信息安全产业高质量发展的若干政策（征求意见稿）》和2020年4月《长沙市关于加快网络安全产业发展若干政策实施细则》，从产业创新、应用示范、园区发展等方面落实整体部署和激励措施，大力促进地区网络安全产业高质量发展。

（二）产品体系逐步完善

1. 我国网络安全产业技术布局相对完整

随着网络安全行业的迅猛发展，现有网络安全产品和服务基本从传统网络安全领域延伸到了云、大数据、物联网、工业控制、5G和移动互联网等不同的应用场景。基于安全产品和服务的应用场景、保护对象和安全能力，我国网络安全产品和服务已覆盖基础安全、基础技术、安全系统、安全服务等多个维度，网络安全产品体系日益完备，产业活力日益增强。网络安全产品/服务图谱如图14所示。



图 14　网络安全产品/服务图谱

2. 网络安全产业链条有待稳固

随着我国网络安全产业近年的高速增长，目前产业链已经逐步完善，供需关系也相对明朗。在产业链上游，我国在芯片、操作系统、数据库、中间件等基础硬件和软件系统方面技术基础仍较为薄弱，在引擎、算法和规则库等基础能力方面则技术能力较为完善。在产业链中游，我国网络安全产品和服务整体发展较为稳固、技术布局相对完整。在产业链下游，党政军、企业用户是网络安全产品和服务主要的消费主体。网络安全产业链如图 15 所示。

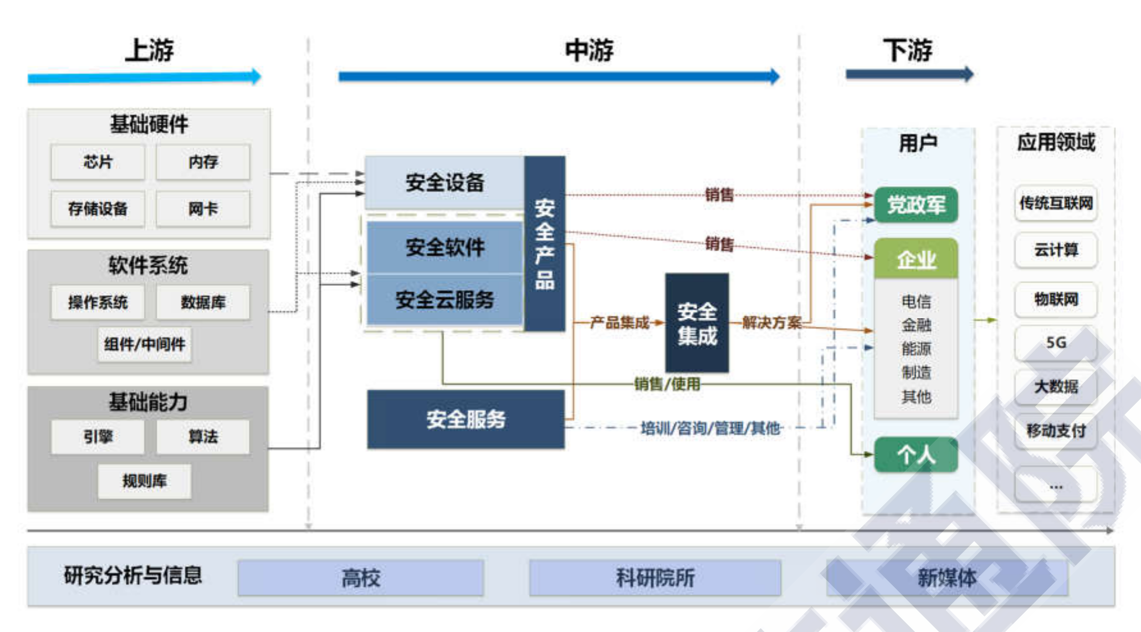


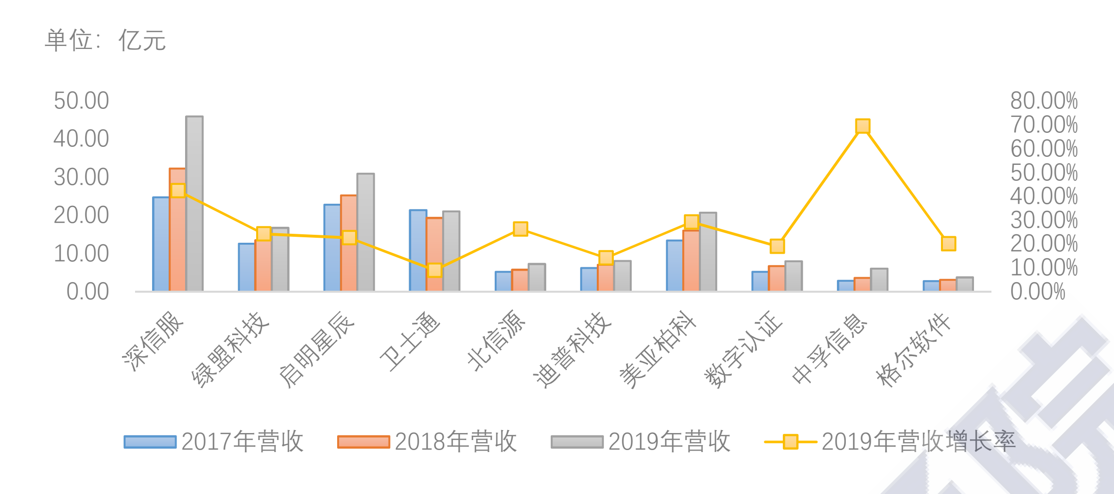
图 15　网络安全产业链

（三）网络安全企业发展总体良好

1. 上市企业业绩稳步增长

在营收规模方面，企业营收规模总体呈稳定增长态势。10 家上市网络安全企业 2019 年平均营收规模为 16.82 亿元，较 2018 年的 13.23 亿元增长了 27.08%。其中，深信服凭借安全业务云化转型实现高速增长，2019 年营收规模首次突破 40 亿元，同比增速超过 40%。中孚信息整体收入快速增长 69%，主要受益于安全服务业务的快速推进。2017-2019 年我国上市网络安全企业营收情况如图 16 所示。

在营业收入构成方面，10 家上市网络安全企业的营业收入主要由网络安全软硬件产品及服务组成；其中，网络安全软硬件产品营收占比较高，平均占比达到企业营业收入的七成。部分网安企业在新兴安全领域的营收迅速增长。2019 年，启明星辰以云安全和工业互联网安全为代表的新安全业务收入约占总收入的 20%，同比增长 200%。



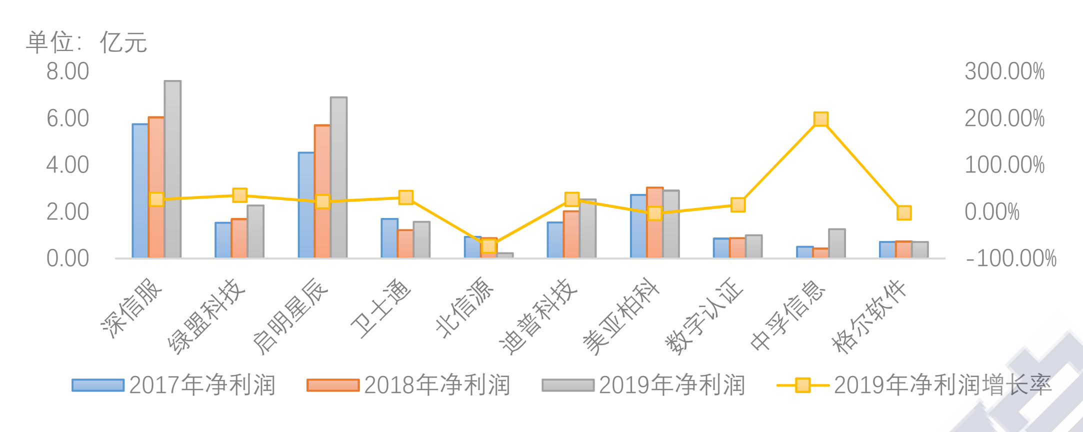
数据来源：中国信息通信研究院（基于上市企业财报整理）

图 16　2017-2019 年我国上市网络安全企业营收情况[30]

在净利润方面，10 家企业平均净利润增速稳步提升，企业盈利能力出现分化。10 家上市网络安全企业 2019 年平均净利润为 2.69 亿元，较 2018 年的 2.25 亿元增长了 19.39%。其中，深信服、绿盟科技、启明星辰和迪普科技 4 家企业的净利润增速稳健，主要源于企业在安全领域的持续深耕和战略化的业务布局；北信源[31]、美亚柏科和格尔软件 3 家企业的盈利能力有所下滑。2017-2019 年我国上市网络安全企业净利润情况如图 17 所示。

[30] 说明：部分上市企业网络安全业务占比较低，故未纳入作为典型企业分析

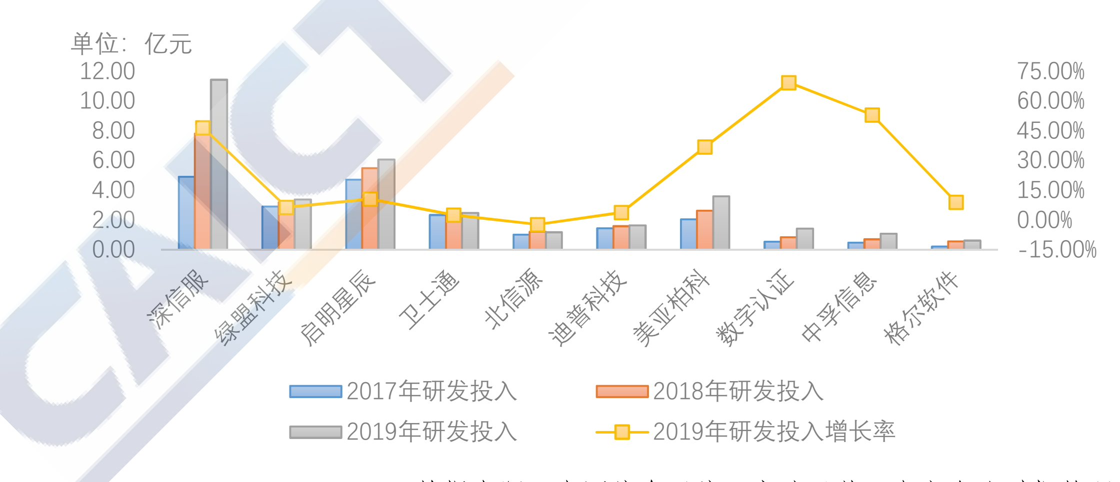
[31] 说明：北信源在 2019 年对应收账款等金融资产计提大额减值损失，导致企业净利润增长率大幅下降



数据来源：中国信息通信研究院（基于上市企业财报整理）

图 17　2017-2019 年我国上市网络安全企业净利润情况[32]

在研发投入方面，企业持续加大研发投入力度。2019 年国内 10 家上市网络安全企业平均研发投入为 3.28 亿元，相较于 2018 年的 2.63 亿元增长了 24.49%。其中，北信源受净利润下降影响，用于研发的投入较上年下降 2.27%。数字认证 2019 年研发投入大幅增长 69.15%，主要用于电子签名应用、电子合同以及信步云等项目研究。2017-2019 年我国上市网络安全企业研发投入情况如图 18 所示。



数据来源：中国信息通信研究院（基于上市企业财报整理）

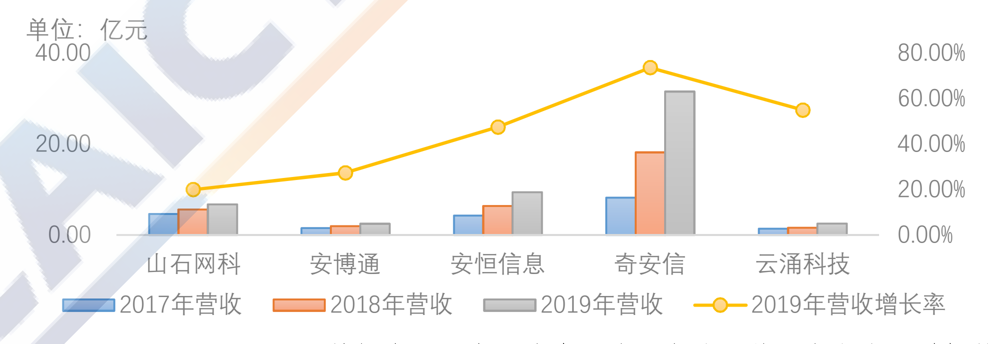
图 18　2017-2019 年我国上市网络安全企业研发投入情况

2. 科创板上市企业发展态势强劲

[32] 说明：部分上市企业网络安全业务占比较低，故未纳入作为典型企业分析

科创板为具有成长性和持续经营能力的网络安全企业提供了新的融资渠道和规模扩张机遇。截至 2020 年 7 月，科创板已上市的网络安全相关企业共计 5 家，分别为安恒信息、山石网科、安博通、奇安信和云涌科技。另有信安世纪等众多优质企业正在进行科创板上市准备。5 家科创板上市企业 2019 年平均营收规模为 10.54 亿元，较 2018 年增长 56.12%。我国在科创板上市网络安全企业 2017-2019 年营收情况如图 19 所示。

2020 年奇安信和云涌科技陆续登陆科创板。奇安信实际募资达 57.19 亿元，创同类型企业 A 股募资额新高，所募集资金将用于建设云和大数据安全防护与管理运营中心、工业互联网安全服务中心等。与同类企业相比，奇安信成长速度较为领先，但是由于选择了高研发投入且人员快速扩张的发展模式，近三年均处于亏损状态。云涌科技成立于 2004 年，业务聚焦于工业信息安全，是电力领域工业信息安全核心设备供应商。



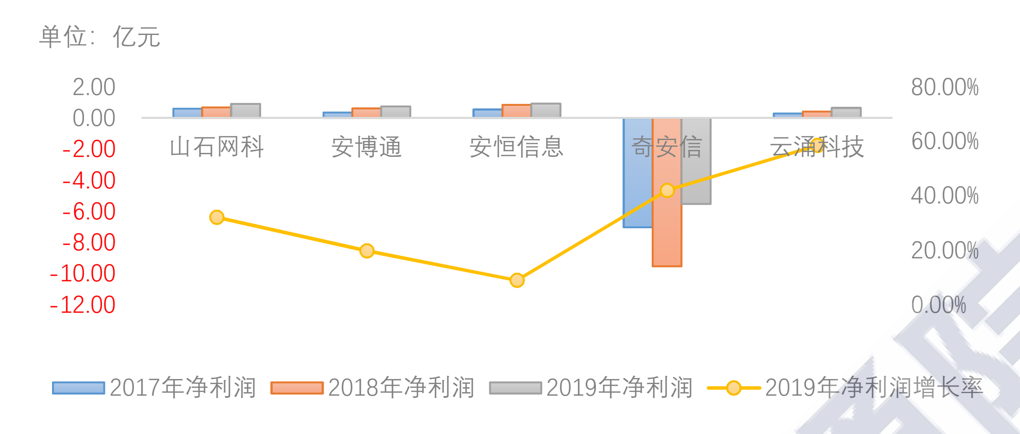
数据来源：中国信息通信研究院（基于上市企业财报整理）

图 19　科创板上市网络安全企业 2017-2019 年营收情况

在净利润方面，4 家[33]科创板上市企业 2019 年平均净利润为 0.81 亿元，较 2018 年增长 26.56%。我国在科创板上市网络安全企业 2017-

[33] 说明：奇安信盈利及增速情况在行业中较为特殊，故计算平均净利润时未将其纳入

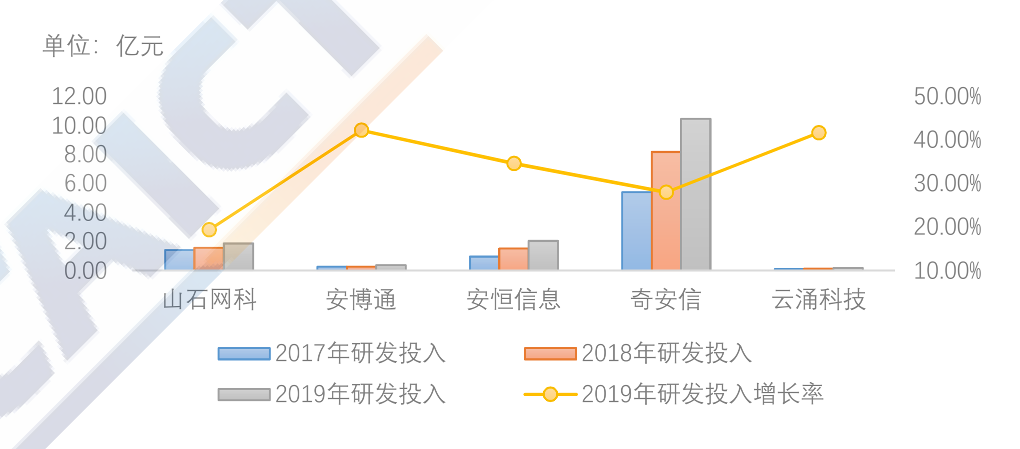
2019 年净利润情况如图 20 所示。



数据来源：中国信息通信研究院（基于上市企业财报整理）

图 20　科创板上市网络安全企业 2017-2019 年净利润情况

在研发投入方面，5 家科创板上市企业 2019 年平均研发投入达到 2.99 亿元，较 2018 年增长 28.16%。从研发项目看，各企业紧跟网络安全行业的创新趋势，将云安全、数据安全、移动安全和工控安全、物联网安全产品的研发作为重点。我国在科创板上市网络安全企业 2017-2019 年研发投入情况如图 21 所示。



数据来源：中国信息通信研究院（基于上市企业财报整理）

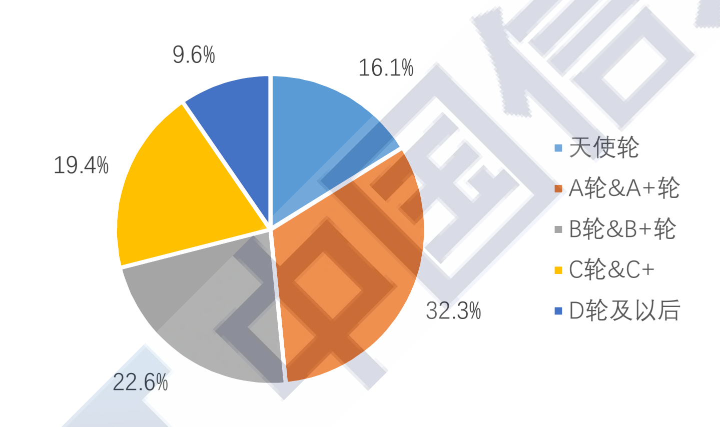
图 21　科创板上市网络安全企业 2017-2019 年研发投入情况

（四）网络安全市场持续激发投资热情

1. 网络安全融资活动持续活跃

据不完全统计，排除股权转让、并购及 IPO 的影响，2019 年中国网络安全行业投融资事件达 40 余起，涉及金额超过 90 亿元。其中奇安信在 2019 年有两次大额融资活动，对融资总额影响较大。

在融资轮次数量分布方面，我国网络安全融资比较青睐早期融资项目。如，早期项目（天使轮-A+轮）数量占比最高达到 48.4%，中期项目（pre-B 轮-B＋轮）和后期项目（C 轮及以后）数量占比分别约为 22.6%和 29.0%，如图 22 所示。



数据来源：中国信息通信研究院（基于公开信息整理）

图 22　2019 年我国网络安全领域投融资分布情况

在融资领域方面，安全服务与新兴领域成为投融资热点方向。如，安全服务领域融资数量最多，达到 14 起，融资总额超过 15.3 亿元；工业互联网安全和物联网安全、数据与应用安全、身份安全融资数量分别达到 9 起、6 起、5 起，位列第二、第三和第四。

在投资参与者方面，投资机构仍然是市场中的主力军，由投资机构领投的项目数量约占总数的 90%；企业/集团领投项目则在涉及金额上展现出巨大能量，约占总额的 46.6%。

2. 大型企业深度布局安全市场

一是安全企业通过收购进行版图升级和拓展。2020 年 6 月，360 全资收购瀚思科技，将充分发挥双方安全能力，共筑安全大脑，推进 360 大安全战略；2020 年 5 月，网宿科技拟以 8 亿元收购创而新教育科技，通过了解教育信息化业态发展情况，挖掘特定应用场景的 CDN[34]、云安全、IDC[35]等网络基础服务定制化需求。**二是重要行业厂商加速网络安全能力布局**。2019 年 10 月，阿里云全资收购九州云腾与长亭科技，其中，九州云腾将补充阿里云在云原生安全能力上的布局，长亭科技将提升阿里云的大型政企客户定制化安全服务能力；2020 年 3 月，中国第一汽车集团旗下的一汽富晟实现对物联网安全厂商信长城的投资，积极布局智能网联汽车、V2X[36]安全等领域。**三是大型国企多线布局网络安全领域**。继 2019 年 8 月中国电子科技集团公司（简称“中电科”）实施股份增持，成为绿盟科技第一大股东之后，同年 11 月，中电科继续入股南洋天融信成为南洋股份的第三大股东，持续完善网络安全领域布局。

（五）新冠疫情对网络安全产业发展造成一定冲击

2020 年新冠疫情席卷全球，我国网络安全产业与其他软件业、服务业相似，由于现场技术服务和招投标项目等进度受阻，产业收入、利润、人员工资短期内出现大幅下降。但随着政策持续加码，长期来看不会影响网络安全产业持续上升的发展趋势。

---

[34] CDN：Content Delivery Network，内容分发网络

[35] IDC：Internet Data Center，互联网数据中心

[36] V2X：vehicle to everything，车用无线通信技术

1. 短期内，产业整体受到一定不利影响

一是新冠疫情影响网络安全产业供需格局，安全业务营收较去年同期明显下降。产业供给方面，上游原材料、芯片厂商停工停产，物流运输不畅等因素导致部分网络安全产品产能下降；现场安全服务无法开展，网络安全服务输出能力减弱。**产业需求方面，**制造业等客户受疫情影响较大，客户本身的经营困难间接影响到安全市场，政府、电信、金融等领域延缓采购计划，也将影响市场。根据工信部软件业经济运行情况监测数据，上半年信息安全产品和服务共实现收入 520 亿元，同比下降 2.6%（上年同期为同比增长 10.8%）。**二是受到人员聚集管控影响，技术交流受限。**2020 年 2 月，仅奇安信、绿盟、山石网科、360 等七家中国企业参展 RSAC2020[37]。随着国际国内的网络安全会议启动在线模式，产业合作与交流减缓，产业人才与产品流通不流畅，对产业和企业发展造成一定程度影响。

2. 长期看，产业将保持持续增长趋势

一是政策持续加码，助推产业回暖。疫情爆发后，中央和地方密集出台 800 项政策，围绕为企业减负、加大金融支持、增加财税补贴、优化政府服务等方面，推动企业发展。疫后政策加码新基建，更为产业发展带来新机遇。**二是安全服务从线下转向线上，服务模式转型有利于降低成本。**受疫情防控影响，远程安全服务业务逐渐增多，如远程安全运维、远程安全测评等，一定程度上也降低了安全企业及其客

[37] RSAC2020：2020 RSA Conference，2020 RSA 信息安全大会

户的成本。**三是云化、远程化等需求激增，为产业带来商机**。随着云化、远程化办公的增长，疫情防控支撑系统、在线教育、远程办公、远程会议等系统和应用大规模推出，网络安全产品和解决方案需求相应增加，智能化、远程化的安全运维需求也逐步提升。

3. 国家重大安全事件应急的启示

一是疫情防控期间个人信息收集与利用问题凸显，数据安全将成为未来网络安全重点关注。疫情防控期间，公共服务行业、运输业以及居民小区等开展的人员信息登记，各类 APP[38]记录的人员导航定位数据、支付数据，在支撑有关部门精准施策发挥了重大作用，但同时授权不清晰、使用不透明、过度及重复采集等数据安全问题十分突出。据中国信通院统计，涉疫情个人信息遭泄露事件占疫情期间数据安全事件总数的 70%左右。目前《数据安全法》和《个人信息保护法》立法工作在稳步推进，如何平衡数据利用和数据安全的关系问题备受关注。**二是远程协作等场景将进一步催生身份认证、访问控制的安全需求**。随着远程办公模式日益普及，IT 边界模糊化的相关安全需求，成为企业升级网络安全防护体系的动力，或将为零信任框架等新型网络安全架构带来更多市场空间。

四、我国网络安全生态建设

（一）产业园区建设持续推进

一是国家网络安全产业园建设初见成效。国家网络安全产业园

[38] APP：Application，应用程序

（北京），由海淀园、通州园和经开区信创园三园组成。截至 2020 年 5 月，海淀园主体大楼开工建设、通州园完成揭牌、经开区信创园实现开园，30 家信创领域支柱型企业集中签约入驻信创园，落地项目涵盖软硬件、芯片和集成服务等领域，5G 技术、云计算、云存储等新型基础设施建设项目。**国家网络安全产业园（长沙），**于 2019 年 12 月正式获批，目前基本形成涵盖基础硬件、基础软件、信息安全服务、工业互联网安全等众多领域的产业链条，以及集聚中科院王小云院士等 20 余名专家的国内首个商用密码产业示范基地。2020 年 6 月，该园正式揭牌，并进行首批入园企业和首批引进项目签约。

二是国家安全产业示范园积极促进产业融合发展。2019 年 10 月，合肥高新区等 6 家单位通过工业和信息化部、应急管理部联合组织的 2019 第一批国家安全产业示范园（含创建）评审，其中合肥高新区、株洲高新技术产业开发区、长三角安全产业园将网络安全纳入发展规划，打造区域产业生态区。**合肥高新区，**积极谋划建设“中国安全谷”，依托产业资源汇聚优势，联合高校科研资源，建设网络空间安全校企合作平台，力争到 2025 年，网络安全总产业规模达到 1500 亿元。**株洲高新技术产业开发区**，作为湖南省自主安全计算机及网络安全产业重要制造基地，初步形成了以湖南长城为龙头企业，覆盖基础软硬件、自主可控终端及安全设备的产业链条。**长三角安全产业园**，致力于打造立足南通、面向长三角、辐射全国的长三角网络安全产业高地，目前已挂牌成立信息安全等级保护关键技术国家工程实验室、工业互联网安全分实验室和江苏智慧安全可信技术研究院，将为加快培育自主

创新能力、加强关键技术的突破发展提供载体支撑。

（二）协会联盟持续增进产业自律发展

一是推动网络安全行业自律体系纵深发展。中国通信企业协会通信网络安全专业委员会推进网络安全服务能力评定工作、网络系统运行单位能力评定工作、网络安全防护能力评定工作及信用体系建设工作，其中 2011 年至今共为 120 家单位颁发 192 个网络安全服务能力评定证书，为推动行业健康发展、维护市场秩序等方面发挥了桥梁纽带作用。**二是疫情期间积极开展网络安全交流活动**。中国网络空间安全协会通过线上举办“未成年人网络安全保护社会评议会--未成年人在线教育平台的网络安全保护”和“新冠疫情下网络空间国际治理新动向”研讨会等方式，为国内专家和行业代表分享交流提供平台。**三是积极引导和支持行业有效承担社会责任**。中国互联网协会关注未成年人网络保护及网络信息治理，不断完善相关举措，推动《网络运营者针对未成年人的有害信息防治体系框架》和《针对内容安全的人工智能数据标注指南》等标准形成和落地。

（三）国家层面积极推动网络安全国际合作

一是加速推动与东盟国家的网络安全合作。2019 年 10 月，中国—东盟网络安全交流培训中心正式揭牌，致力于加强中国与东盟国家在网络安全方面的交流合作，共同提高网络安全水平。2019 年 11 月，我国在第 22 次中国-东盟（10+1）领导人会议上呼吁推动双方在数字经济、人工智能、大数据、网络安全等领域开展创新合作。**二是加强**

关键领域的国际合作。2019 年 10 月，世界互联网大会组委会发布《携手构建网络空间命运共同体》概念文件，文件就加强关键信息基础设施保护和数据安全国际合作、及时共享网络威胁信息并有效协调处置重大网络安全事件等方面提出倡议。**三是为加强全球数字治理贡献中国智慧。**2020 年 9 月，在“抓住数字机遇，共谋合作发展”国际研讨会上，中方提出《全球数据安全倡议》，提倡尊重他国主权、不侵害个人信息的数据安全原则，强调各方应在相互尊重基础上，加强沟通交流，深化对话与合作，共同构建和平、安全、开放、合作、有序的网络空间命运共同体。

（四）需求推动人才培养多管齐下

2019 年(ISC)² 网络安全劳动力研究报告[39]显示，网络安全人才缺口仍在扩大。全球方面网络安全劳动力缺口 127 万，需在现有 280 万的基础上增加 45%，才能够满足日益增长的网络安全专业人员需求。面对当今严峻的人才短缺形势，各国全力应对，在院校培养资源受限的情况下，积极通过演练、教育和培训、组建网络安全战略联盟等手段，基于网络安全学习平台、虚拟网络学校等载体，探索网络安全人才培养新途径。

为了助力应对未来人才挑战，我国多措并举，不断完善网络安全人才培养机制。**一是以赛代练，网络安全竞赛擂鼓呐喊。**2019 年 10 月，“护网杯”2019 年网络安全防护赛暨第二届工业互联网安全大赛在北京闭幕，共有 6479 支队伍、15000 余名选手参赛。11 月，第六届

[39] 数据来源：(ISC)²，2019 Cybersecurity Workforce Study，2019

电信和互联网行业网络安全管理职业技能竞赛全国决赛在西安举行，竞赛历时 6 个月，覆盖全国 31 个省份、1.2 万人参与。2020 年 8 月，中央企业“新基建”网络安全技术大赛开启报名，选拔符合“新基建”发展的新型网络安全人才。**二是资源整合，人才培养基地融合创新。**2019 年 5 月，亚信安全与中国信息通信研究院共同成立 5G 安全协同创新中心，推动 5G 安全技术创新、人才队伍建设；2020 年 7 月，江苏省网络空间安全（无锡）实训基地落成启用，将充分发挥基地示范和带动效应，有望成为网络安全人才发展的“新摇篮”。**三是平台效应，网络安全大会助推产业发展。**2019 年 9 月，网络安全宣传周在天津盛大举行，110 余家互联网、网络安全企业参展，参观人数达 14.5 万人；2020 年 6 月，“2020 西湖论剑·网络安全线上峰会”成功召开，聚焦后疫情时代的网络安全新业态、新模式，系统解读数字中国发展浪潮中的新兴安全领域最新成果；2020 年 8 月，360“互联网安全大会”、奇安信“北京网络安全大会”先后开幕，采取“线上”云会议形式，国外内业界重磅嘉宾助阵，盛况空前。**四是在线培训，公益课程云上开课。**2020 年 2 月，360 网络空间安全教育云平台上线网络安全培训公益课程；2020 年 3 月起，中关村可信计算产业联盟连续举办多期网络安全线上直播课程；2020 年 5 月，工业和信息化部指导工业和信息化部人才交流中心设立了网络安全在线培训平台。

五、我国网络安全产业前景展望

（一）核心技术突破驱动安全能力发展

为了在新基建建设过程中强化网络基础设施的安全保障，加强核心技术攻关，促进供应链安全发展，推动产业链上下游整合成为当前发展的主题。**一方面**，在我国对技术创新支持力度不断提升的大背景下，产业链各环节相关主体将持续加大在关键核心技术方面的研发投入，形成以企业为核心的产学研用创新主体并开展科研攻关，实现核心技术突破、产业能力提升、产业生态健康发展。**另一方面**，对安全防护而言，产业链条中任何一个环节的弱点和漏洞都可能成为防护的短板，为寻求安全能力的整体提升，安全厂商将与产业链的各环节进行深度融合，实现上中游的无缝衔接，从源头出发打造全链条的更具内生安全能力的安全生态。

（二）产业合作发展成为趋势

一方面，随着国家级产业园区建设的逐步提速，依托高校、企业、联盟等网络安全产业基础，北京、长沙、合肥等多个城市大力推进网络安全集聚发展，加强资源整合和政策引导，促进政策、技术、产业和人才等要素之间的良性互动，为产业合作构建良好生态体系。**另一方面**，打破不同网络安全企业主体间数据孤岛、增进手段联动的需求日益迫切，诸如借助网络安全威胁信息共享、集中处置等技术手段，进一步整合网络安全不同企业主体间的技术优势、资源优势，破解当前建设分散、投入重复、资源壁垒的问题。

（三）线上培训开辟人才培养新路径

疫情发生以来，政府部门、高等院校、行业联盟、安全企业等为

了解决我国网络安全人才数量和能力缺乏等问题，积极结合自身优势与资源，通过开展在线的网络安全培训、竞赛，线上或线上与线下结合的网络安全会议等方式，探索人才培养与交流的新路径，助推了人才工作的数字化转型。人才培养“云”模式将为推动基础人才培养、促进高端人才交流、加速国际合作、引进海外人才等创造更加高效便利的途径。

（四）新兴领域与重要行业政策将持续细化明确

新基建与信息化建设的持续推进，在驱动经济和产业模式变革的同时，也将对网络安全保障提出更高要求，从而进一步推动相关支撑政策加快落地。**一是新兴领域安全保障政策将逐步完善。**随着网络安全建设与信息化建设逐渐同步，相配套的网络安全基础设施以及网络安全保障体系变得越发重要，为了保障 5G、大数据、人工智能、工业互联网、物联网等领域的稳定发展，各领域网络安全保障相关政策标准将随着实践的推进进一步完善。**二是重要行业的安全要求将向精细化方向发展。**以数据安全为例，《中华人民共和国数据安全法（草案）》的出台将为数据安全管理等提供更多顶层设计，但是由于垂直行业数据采集和管理方式不尽相同，数据流量类型千差万别，数据安全保障需求各异，形成以行业为导向的数据安全管理规则将成为大势所趋。目前，金融、工业等重要行业已陆续出台数据管理指引，预计未来与行业相结合的安全政策将会持续落地。

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62304839、62300128

传真：010-62304980

网址：www.caict.ac.cn

